SAIC®
An Employee-Owned Company

Telecommunications and Networking
Systems Operation

1710 Goodridge Drive
McLean, Virginia 22102

ORGANIZATION AND BUSINESS CASE MODEL
FOR
INFORMATION SECURITY

26 AUGUST 1997

Submitted to:
Office of the Manager,
National Communications System (OMNCS)
Customer Service and Information Assurance Division
Information Assurance Branch (N53)

Prepared by:
Science Applications International Corporation (SAIC)
Telecommunications and Networking Systems Operation
Under Contract No. DCA100-95-D-0104
Delivery Order 10

OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

ORGANIZATION AND BUSINESS CASE MODEL
FOR
INFORMATION SECURITY

26 AUGUST 1997

**Further distribution only as directed by the
Office of the Manager,
National Communications System (OMNCS)
Customer Service and Information Assurance Division
Information Assurance Branch (N53)**

TABLE OF CONTENTS

LIST OF EXHIBITS

EXECUTIVE SUMMARY

The purpose of the project was to develop a business-based approach/methodology for justifying funding for information systems and network security expenditures. The project included research and analysis of four individual case studies (three public sector telecommunications companies and one Federal agency). The case studies are based on past experiences of business interruptions or losses owing to a lack of, or installation of ineffective, security measures.

The hypothesis of the project is that significant security incidents have provided motivation for security investments and that a reasonable proactive security investment would have mitigated the effects of the incident, resulting in a lower overall cost. While the research did not support the hypothesis, analysis of the case study observations, results, conclusions, and supplemental research provided two prevalent themes. Organizations react to a variety of motivations for security investments, not just return on investment, and significant security investments (generally over $1 million dollars) are subject to the rigors of a business case justification □ as are all other significant investments. In the absence of a single network intrusion, related service denial, or security incident which might provide a broadly applicable motivation for security investments, SAIC proposed that a model for information security investments be used to provide that motivation. The proposed model takes into account and is organized on the basis of the two prevalent themes. The organizational model is discussed in terms of an ideal organizational climate from the standpoint of information security and in terms of the structure and process used to determine and approve security investments. The business case model is discussed from the standpoint of traditional business case models with a view toward incorporating non-traditional motivations and emerging concepts for return on investment.

The report also concludes that:

- Companies do not generally attempt to capture the costs of recovering from network intrusions and other security incidents. The primary motivation for capturing these costs would be to establish a dollar value threshold of loss in order to seek legal recourse (e.g., charge and prosecute a perpetrator or file a civil suit).

- Network intrusions and other security-related exposures or incidents alone are not sufficient to provide the focus and motivation needed for long-term security solutions. Security programs driven solely by a “big” security incident or intrusion eventually fade away because the motivation for the program □ the incident or intrusion □ is forgotten and funding for the program is no longer justified in the eyes of senior management.
- A proactive capability to deter, detect, and contain security incidents in conjunction with adequate protection measures minimizes losses in revenue and customer confidence.
- The relative size of each entity’s information security program was found to be directly proportional to the number of external customers served by the entity.
- With few exceptions, the stakeholders [1], board of directors, and senior management historically were unaware of the risk exposure caused by information security (INFOSEC) incidents and accidents.
- Strong, multidisciplined business assurance audit programs with senior management involvement and support across the entity are extremely helpful in assessing and managing overall risk.

[1] Throughout this discussion, the term “stakeholder” is used. It is an inclusive term that encompasses stockholders in the commercial sector. Being a broader term, it addresses similar constituencies in the not-for-profit and the public/government sectors. In addition, there is a range of stakeholders in each organizational entity, identifiable by their place and their role in the decision process.

SECTION 1
INTRODUCTION

1.1 BACKGROUND

In recent years, information and telecommunications technology and services have expanded at an astonishing rate. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological change, public and private organizations are undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and, at the same time to compete in a global marketplace. Even during prosperous economic times, security has not been easy to sell to senior management unless the organization has recognized that it has been the victim of a major security incident. In today's business environment it is difficult to obtain senior management approval for the expenditure of valuable resources to "guarantee" that a potentially disastrous event will not occur that could affect the ultimate survivability of the organization.

Science Applications International Corporation (SAIC) was tasked by the Office of the Manager, National Communications System (OMNCS), Customer Service and Information Assurance Division, under the Defense Information Systems Agency (DISA) contract DCA100-95-D-0104, Delivery Order 10, to provide the Government with a report supporting the justification of funding for network security-related programs.

The overall purpose of this project was to develop a business-based approach/methodology for justifying funding for information systems and network security expenditures. The project included research and analysis of four individual case studies that are based on past experiences of business interruptions or losses owing to a lack of, or installation of ineffective, security measures. Each case was analyzed to identify business approaches that could be generalized and used as the basis of a methodology for justifying proactive security funding.

1.2 APPROACH

The research team compiled a list of potential case study candidates that either had experienced a significant intrusion or had initiated a security program to address other competitive business or environmental concerns. From this list of potential candidates, three were selected for analysis by the Government Technical Task Manager. The fourth case study was added as a target of opportunity when an organization revealed interest in participating in the case study process.

The case study points of contact were notified and non-disclosure agreements were executed to protect the anonymity of the case study participants. Each case study was also assigned a code name. Meetings and interviews were scheduled with the key officials within the organization and guided by questionnaires developed for each case study participant. Relevant data was collected to include copies of policies and procedures, incident summaries, business case procedures, organizational flow charts, and other relevant information. Data was also supplemented with open source material from the media and Internet sources such as corporate home pages, etc.

The research team wrote case study reports based on the interviews conducted and data collected and distributed the reports to the case study point of contact to review for factual accuracy. The case studies were then analyzed in conjunction with literature reviews and surveys to develop a business case model for security investments. The end result is a synthesis of the best components of the four case study security programs. The research team used this synthesis to create a business model for security investments on the basis of tangible and intangible cost/benefit considerations.

This final report is a recommended approach for justifying security funding. The approach is based on the best practices of the case studies as modified by supplemental research and analysis.

1.3 ORGANIZATION OF THE REPORT

Section 2 of this report summarizes the four case studies conducted as part of the research and offers conclusions based upon these case studies. Section 3 presents a summary of supplemental research of open literature on industry trends in information security, including an examination of recent information security surveys. Section 4 offers an information security business model based upon lessons learned and best practices from the case studies and supplemental research. Section 5 presents lessons learned and suggests future research areas.

SECTION 2
ANALYSIS OF CASE STUDIES

Four organizations were extensively interviewed and researched as part of the case study component of this project. Detailed case study reports were submitted to OMNCS under separate cover for distribution at the discretion of the OMNCS. Section 2 briefly summarizes the case studies within the format followed in the detailed case study reports.

The costs identified in the case studies are presented in Section 2.5.2 and therefore excluded from the summaries presented below.

2.1 CASE STUDY 1, CODE NAME SEBRING

SEBRING is a multi-billion-dollar telecommunications, information, and entertainment services company. SEBRING is moving from an old centralized mainframe computer system to a new distributed client-server environment for its customer services and its own internal use.

2.1.1 Motivation for Program

The establishment of a security program at SEBRING was motivated by several significant factors, which included interest shown by the Board of Directors, increased competition, and peer experiences.

Of the motivating factors, the most compelling was the Board of Directors' interest in the program. A briefing regarding a recent security incident was presented to the Board of Directors. This briefing sparked interest in the security program and garnered the support of the Board of Directors. In fact, this briefing resulted in a member of the Board of Directors becoming a "champion" of the Board for the Security Program.

2.1.2 Security Program and Interfaces

The Security Program at SEBRING consists of a small group of security professionals (two to four staff members) who, in addition to security, are also responsible for business continuity. The director of the program reports to the Director of Information Technology (IT) Operations, who reports directly to the Chief Information Officer (CIO). The director of the program has established an interface with senior management as a result of peer pressure, to keep the program visible to the Board of Directors. The director of the program also has a good liaison with the Vice President of Internal Audit and informal liaison with the business units, and participates in an informal security committee.

The director of the security program interfaces with industry organizations and belongs to the Telecommunications Security Awareness, Research and Standards (TSARS) (Regional Bell Operating Companies [RBOCs] and clients) and International Information Technology Users Group (IITUG).

2.1.3 Policy and Procedures

Security policies and procedures are in place, and are currently undergoing revisions to reflect the changing technological and business cultural environment. The policies also include an information classification program for protecting SEBRING information.

2.1.4 Business Case Model

SEBRING uses detailed business case decision support documentation for projects over $1 million. The business case procedures include a detailed methodology and approach. No business case procedures are in place specifically for security investments or in support of funding for the security program in general.

2.1.5 Senior Management Views

Security is an area of great concern to SEBRING senior management because of its high visibility to the Board of Directors and because of increased media coverage of SEBRING's operations. SEBRING acknowledges that investment in security is part of the cost of doing business and views outsourcing to vendors as part of the solution.

2.2 CASE STUDY 2, CODE NAME EL DORADO

EL DORADO is a government agency using high technology with a large and varied workforce involving a large research community. EL DORADO is broadening its centralized mainframe computer environment into a widely diversified, highly distributed client-server, supercomputer, and extensively networked environment required for its research pursuits and operational needs.

2.2.1 Motivation for Program

Initial security considerations at EL DORADO were motivated by military classified missions and the security compliance programs associated with the classified environment. However, after the classified mission was removed from EL DORADO, a software integrity issue prompted Congressional interest and a security review that served as the basis for the development of a risk-based security program. Other motivations include ongoing security incidents and the need to comply with Office of Management and Budget Circular A-130.

2.2.2 Security Program and Interfaces

The security program at EL DORADO consists of a small, centralized professional staff of six with no future growth or reduction anticipated. The entire program is now staffed with government employees instead of commercial contractors. The Center Computer Security Manager reports directly to the EL DORADO CIO.

The security program interfaces internally with the representatives from the Center directorates through an internal security committee. The program also conducts anecdotal awareness briefings throughout the center. Externally, the program sponsors participate in an Agency-level IT Security Working Group.

2.2.3 Policy and Procedures

EL DORADO security policies are risk-based rather than compliance-based and include an information valuation program. EL DORADO security policies are currently being updated to reflect the changing technological environment.

EL DORADO also has an excellent awareness program that includes internal anecdotal briefings. These are based on actual incidents that demonstrate the need for a security program and security awareness in all levels of the EL DORADO organization.

2.2.4 Business Case Model

EL DORADO does not require the use of a specific business case or economic methodology in its security program. EL DORADO does, however, require that line managers for sensitive applications and data processing installations perform risk analyses to enable them to make informed decisions about the acceptability of risks.

2.2.5 Senior Management Views

EL DORADO senior management notes that incidents serve as reminders that the safety of all elements (especially personnel) of the Center is the top priority. Senior management acknowledged that the transition from a compliance-based program to a risk-based program required a change in mindset and detailed justification for security expenditures. Senior management viewed the outsource vendors as a significant and traditional component of the EL DORADO team that present no unique security risks.

2.3 CASE STUDY 3, CODE NAME SCOUT

SCOUT is a U.S.-based international telecommunications, Internet, and information services company that provides services to business and residential customers across the country.

2.3.1 Motivation for Program

The establishment of the SCOUT security program was motivated by the tremendous growth and change in the business environment, including increased competition, risk, and connectivity. Recurring security incidents motivated the concept of a deter-protect-detect-contain capability that was eventually realized through the creation of the Proactive Security Program (PSP).

The PSP demonstrated the ability to prevent, detect, and contain incidents that would have been very costly for SCOUT. Resources and public image have also served as motivation for the maintenance and growth of the security program.

2.3.2 Security Program and Interfaces

The security program at SCOUT is of medium size and contains 13 staff professionals, 3 to 5 of which are dedicated to PSP activities. The director of the program reports directly to the Chief Financial Officer (CFO)/Chief Operating Officer (COO), as well as to the Chief Executive Officers (CEOs) of each SCOUT subsidiary.

Internally, the director has an excellent interface with senior management and internal audit. PSP interfaces with all of SCOUT's business units. Externally, the director of the program participates in various security and industry groups.

2.3.3 Policy and Procedures

SCOUT currently has policies in place that include an information classification program. The policies are currently being updated to provide more detailed definitions of areas such as “unauthorized use.” SCOUT policies and procedures are closely linked with corporate goals.

An employee separation program was highlighted during the research visit that exemplifies cutting-edge policies and procedures in this area. PSP procedures for rapid response to incidents provide containment and minimize the exposure and risk of any given incident.

2.3.4 Business Case Model

Major investments beyond $1 million require a detailed business case. Less formal decision support documentation is required for system upgrades and cost reduction measures (e.g., access control for central offices).

2.3.5 Senior Management Views

SCOUT senior management stressed the importance of the open interface between the security director and senior management to ensure effective dialogue. Loose links with corporate compliance programs were also discussed. The Telecommunications Act of 1996 brought about many changes in interconnection and unbundled access. Senior management was especially concerned that the changes may place SCOUT at greater risk of affecting the information related to their installed base of customers and services.

2.4 CASE STUDY 4, CODE NAME AMBASSADOR

AMBASSADOR, originally a local telephone company, is a worldwide telecommunications company with a diverse range of information processing systems. Today, AMBASSADOR's local, long-distance, Internet service provider, and wireless subsidiaries provide integrated communications services to millions of customers nationwide.

2.4.1 Motivation for Program

The major motivation for the AMBASSADOR security program was a non-security-related outage. The investigation of this outage uncovered significant security deficiencies. Internal audit findings, ongoing incidents, and customer privacy considerations also provided motivation for the program. In addition, the Federal Sentencing Guidelines, revised to reflect changes in the federal computer fraud and abuse statute, provided additional support and motivation for AMBASSADOR's security program. These guidelines, which become effective November 1, 1997, "can multiply fines as much as 400% or reduce them by up to 95%, depending upon specific factors, **many of which partially depend upon how an organization has responded to the guidelines prior to the violation**. Thus, a company could be fined between $250,000 and many millions of additional dollars, depending upon whether it played an active role in promoting the crime and its degree of cooperation with the Government. In addition, there is a possibility for a shareholder suit alleging that the directors and officers were negligent in not taking the simple but important step of developing an effective compliance program that could have saved the company from these problems (and costs)." [2]

[2] Sherizen, Sanford, *Federal Sentencing Guidelines: An Update on Important New Information Security Liabilities*, Data Security Systems, Natick, MA, 1997, page A-5 (attached as Appendix A to this report).

2.4.2 Security Program and Interfaces

The AMBASSADOR security program consists of 38 professionals with anticipated near-term growth to encompass business function expansion. The security program is responsible for corporate-wide information, network security, and disaster recovery planning and recovery.

The Executive Director of the program reports directly to the CIO. The Director also has an excellent interface to the Corporate Compliance Officer for Oversight and Reporting and an adequate informal liaison with all of the AMBASSADOR business units. Externally, the Director is a member of various industry and security forums, including TSARS. In addition, the CIO and the Executive Director provide direct support for the information security policy, programs, and systems conducted by Public Switched Network (PSN) network personnel.

2.4.3 Policy and Procedures

Security policies are in place and were recently updated to address system life-cycle issues and expanded employee responsibilities. Policies and procedures exhibit significant concern about customer privacy, business continuity, service outages, and incidents. There is a hotline for reporting, and AMBASSADOR outsources some investigative services to the Bellcore Forensics Lab. All policies and procedures are subject to audit.

2.4.4 Business Case Model

AMBASSADOR requires a formal quantitative business case analysis for expenditures over $1 million. A “Big Eight” accounting firm developed a business case recently for a $10 million Disaster Recovery and Information Assurance project for data centers on the basis of business impact analysis.

2.4.5 Senior Management Views

Information assurance is a necessity in today's competitive, customer-focused business environment. Outsourcing critical infrastructure operations, including security, and the changing nature of the marketplace are part of the security problem. The security approach is closely coupled with Corporate Code of Conduct and legal compliance programs (e.g., U.S. Sentencing Guidelines). Internal Audit provides a healthy self-analysis of business assurance with respect to security. Stakeholders, management, and oversight understanding of the risk are key to solving the problem before it becomes a marketplace or regulatory event.

2.5 OBSERVATIONS, RESULTS, AND CONCLUSIONS

2.5.1 Observations

In general, the case studies showed:

- Trusted relationship between research team and case study candidates was required even to persuade companies to participate.
- Participating companies were very cooperative.
- Security departments are treated as cost centers and not profit centers.
- Security funding is a "cost," not an "investment" .
- Security costs are generally allocated to business units.
- Incident costs are not captured.
- Many intruders are not prosecuted.
- Malicious employees are terminated without prejudice.

2.5.2 Results

Exhibit 2-1 summarizes the results of data collection associated with the case study incidents.

	SEBRING	EL DORADO	SCOUT	
Incident(s)	Network Intrusion (Rootkit and Trojan horses installed into Internet firewall server to Corporate backbone network).	Unauthorized Software Modifications	1. Denial of Service Attack (TCP SYN)	2. Insider Attack - Wor Stoppage (changed BIO passwords to Corporate systems).
Action	Detected by independent intrusion analysis. Briefed Corporate Board. Focused and helped initiate new security activities in an outsourced environment. Established Director of Network and Information Security and small staff (three) and expectations on security testing and closure.	Detected because of heightened security concerns following Challenger accident. Independent security review revealed vulnerabilities. Established enterprise-wide enhanced security program.	Detected and contained by Proactive Security Team (PST), referred to Federal Bureau of Investigation's (FBI's) National Computer Crime Squad (NCCS) for possible prosecution.	Detected rogue passwor changes, identified perpetrator(s), reset syst Largest disciplinary acti date for work stoppage-r acts. Incident served as significant deterrent to f acts of sabotage.
Costs	$40,000/Yr. for Bellcore support.	N/A	N/A	N/A
Investigation	$6,000 additional for incident.	$5,000 □ Independent review.	$9,000 □ PST labor.	PST costs not collected l SCOUT.
Outages	Potential for significant outages.	Unknown. Unable to perform mission (i.e., launch space shuttle).	$13,000 □ Lost service.	Potential for significant but impact minimized b proactive investment an reaction capabilities.
System Recovery	Minimal costs but significant effort. Costs included in Subsequent Investment (Staff).	$450,000 □ 35 member security team. $400K - contractor support to security team.	Potential for significant system recovery costs and lost business, but minimized by proactive investment, swift reaction and deterrent actions to isolate intruder.	Potential for significant losses and recovery cost minimized by proactive investment in reaction a deterrent capabilities, tr and personnel.
Subsequent Investments	$500,000 □ Network Access Control $270,000 □ Smart Cards $240,000/Yr. □ Staff	$325,000/yr. □ Program sustainment staff. $75,000/yr. □ Contractor virus response. $220,000 yr. □ Security tools and software.	Not available.	Not available.
Loss of Shareholder/ Customer Confidence	Incident not revealed to public, but significant enough to spark Board action.	Required to testify to Congress. Potential loss of human life and negative public perception of space program.	Not measurable, but some customer complaints logged.	Incident not revealed to
Increase in Insurance	N/A	N/A	N/A	N/A
Proactive Costs of Security Prior to Incident	Security department with current penetration testing efforts might have identified holes and prevented intrusion.	Substantial based on System Recovery and Subsequent Investment.	Proactive investments significantly minimized cost. (Internet Service provider [ISP] peers under similar attack suffered extensively □ e.g., WEBCOM, PANIX)	Proactive investments significantly minimized

Exhibit 2-1. Summ

2.5.2 Conclusions

2.5.2.1 Motivation for Program

Among the case studies, the greatest motivating factor for the implementation or continuation of a security program is the interest shown by the Board of Directors and/or senior management. Other motivations include customer confidence, competition, peer experience, compliance, business assurance, and changing federal sentencing guidelines.

Security incidents are sufficient motivators and help maintain the program's exposure to senior management, but other motivations must exist to maintain the survivability of the program. Security-related incidents, such as unauthorized or inappropriate use of computer systems, also motivate the establishment of security policies and procedures within the organizations.

2.5.2.2 Security Program and Interfaces

The critical interface for security programs are those that create direct access to the Board of Directors and/or senior management. The survivability of the program depends on sufficient access to senior management within the organization. Interfaces to business units and other internal elements also help solidify incident reporting procedures and other essential distributed functions that rely on an awareness and understanding of the security challenges faced by the organization.

All case study participants maintained an external interface to keep in contact with peers and industry practices, threats, and initiatives. Many use benchmarking, professional associations, and contractual (Bellcore) and federal (law enforcement) support elements.

2.5.2.3 Policy and Procedures

All case study participants have policies in place, including information classification programs, and are currently conducting revisions of their security policies. This indicates that policies in this area need to be updated frequently to reflect the changing technological environment.

Ideally, procedures should be proactive and focus on the full spectrum of information assurance (protect/detect/contain and deny). These procedures should be audited for compliance and procedures should also be in place for policy compliance assessments.

2.5.2.4 Business Case Model

Business case models for *security* are significantly lacking in the case studies. Business case procedures are in place for large expenditures (usually over $1 million), but the analysis uncovered no documentation for establishment or maintenance of security programs.

2.5.2.5 Senior Management Views

Senior management is looking for the issue to be addressed reasonably, effectively, competitively, and in a timely fashion. Security is viewed as a cost of doing business, and does not justify unlimited expenditures. Security programs should be empowered by senior management, and also accountable to it. Management does not like surprises and should be kept informed of all security incidents occurring within the organization.

Senior management should be aware of the technology and open to discussion and education regarding potential security investments to ensure that funds are allocated wisely and in the best interest of the organization.

Exhibit 2-2 summarizes the observations in each case study that led to the above conclusions. In Exhibit 2-2, the code name ESCORT refers to a hypothetical organization whose security program is based on the best practices of the case study organizations. Section 4 presents an organizational and business case model for information security based on these conclusions.

.

Function	Conclusions ESCORT	Case Study #1 SEBRING	
Motivation	Board interest. Compliance. Customer confidence. Business assurance. Competition. Management awareness. Peer experience. Changing sentencing guidelines. Increasing connectivity. Media.	Board requested briefing on incidents. Security champion emerged on board.	Classifie Software interest News m Ongoing Complia
Organization and Interfaces	Size should match the company culture and goals. Proactive and business focused organization is a must □ not auditors!	Very small centralized organization. Security office has business continuity responsibilities. Use informal security committee. Security responsibilities included in outsourcing contracts, including critical public switched network information technology environments.	Small ce Civilian Virus re
Management	Access to senior management and the board is essential.	Director of Security Director of IT Operations CIO	Center CIO
Staffing	Staffing is function of the business environment, stability of the company, perceived risk and value-added nature of security.	Small staff (two). Anticipate growing to four.	Small st
Interfaces	Internal □ Interfaces are critical; must have ability to communicate with board, business units, senior management, systems administrators, data custodians, and all employees. External □ Use benchmarking, professional associations, technical escalation to forensics labs, specialize groups such as the NSTAC NSIE, regulators, law enforcement (SCOUT).	Good interface from senior management because of pressure from board. Good liaison with VP, Internal Audit. Informal liaison with business units. Belong to TSARS (RBOCs and clients) and IITUG.	Internal from Ce Participa group.
Policy	Need continual update. Need clarity of accountability, responsibility, and consequences. Map to Code of Conduct. Update Code of Conduct. Keep it Short and Simple! Must be endorsed by senior management, distributed in multimedia. Must be subject to audit.	Policies in place. Includes classification program. Policies being updated.	Policies Includes Policies Risk ma
Procedures	Need proactive protect-detect-contain and deny capability. Need audit and compliance. Need policy compliance assessment by procedures.	Single point of referral for incidents. Help desk referrals. Outsource firm referrals. Priority of resolution based on severity of incident. Investigate internally or refer to outsource vendors for closure. Use Bellcore Forensics Lab as back-up.	Good aw based on
Business Case Procedures		Reduced business case decision support documentation required for projects over $1 million. Strong methodology and approach.	The mar systems and risk
Senior Management Views	Issue must be addressed reasonably, effectively, competitively, and in a timely fashion. No surprises. Empowerment and accountability. Awareness of technology. Enlightenment. Cost of doing business.	High area of concern, e.g., media. Security is cost of doing business. Viewed outsourcing vendors as part of the team solution.	Incident Transiti was diffi program Viewed unique r

Exhibit 2-2. Case Study

SECTION 3
SUPPLEMENTAL RESEARCH AND ANALYSIS

3.1 DESCRIPTION OF SUPPLEMENTAL RESEARCH

This section outlines the research and analysis conducted to supplement the case studies. This research and analysis was undertaken to provide background for the case studies, to validate some of the findings of the case studies, and to provide additional insights into development of the organization and business case model outlined in Section 4.

3.2 INFORMATION SECURITY SURVEYS

Several surveys regarding information security practices and investments have been conducted in the last 2 years. These surveys provided background information and perspectives for the case studies.

A few observations on the surveys as a whole: first, when security practitioners use certain terms in the reports of these surveys, the exact meaning may not always be the same □ e.g., what constitutes an attack? Second, the basis used for reporting many of the findings in the surveys were similar in some areas and quite different in others. Third, the sizes of the surveys and the areas statistically tracked differed significantly. However, despite these observations, certain trends on lack of security investments, continuing exposure, actual incidents, and general management neglect seemed to be constant in all.

Ernst & Young surveyed 1290 chiefs of information systems, information security officers, and other high-level technology managers in 1995. Exhibit 3-1 shows some of the pertinent results.

- Threats against corporate data are continually rising.
- Corporate information systems are being tied into ever-larger intranets and into the Internet.
- Senior management has done very little to counter the threats.
- Sources of significant financial losses include computer viruses, stolen data, sabotage, network break-ins, network failure, software errors, and computer failures.

Exhibit 3-1. Ernst and Young 1995 Survey Results [3]

In collaboration with *Information Week,* Ernst and Young conducted another survey of 1320 high-level technology managers in October 1996. Results shown in Exhibit 3-2 were reported in *Information Week*.

- Threats against corporate data continue to rise.
- More companies are storing increasing amounts of corporate data on information systems.
- Senior management expressed concern over the threat, but has done very little to counter the threat.
- Very few companies have established a dedicated information security staff.
- Most companies do not have a formal security policy.
- Many companies face problems in procuring skilled information security personnel.
- Most senior managers fail to see information security as “value-added” contribution to “bottom line.”

Exhibit 3-2. Ernst and Young / *Information Week* 1996 Survey Results [4]

The Computer Security Institute conducted surveys in 1996 and 1997 in collaboration with the FBI’s San Francisco-based Computer Crime Squad. The 1996 survey included security practitioners from 428 varied U.S. corporations, government agencies, financial institutions, and universities. The 1997 survey included 563 similar organizations. Exhibits 3-3 and 3-4 show the results of these surveys.

[3] Panettieri, Joseph C., "Security -- The good news", Information Week, November 22, 1995, page 1.
[4] Violino, Bob, “The Security Facade,” *Information Week*, October 21, 1996, page 36.

- Over half of the respondents had intrusions or attempted probes of their internal systems.
- Over half of the respondents did not have a written policy on how to deal with intrusions.
- Most respondents did not have any written instructions on how to preserve evidence of tampering for legal proceedings.
- Most respondents did not have any kind of “Warning” banners on their systems to indicate that they will monitor activities.
- Many respondents did not even know if they have been attacked.
- Industries concerned about security:
  - Banks (60 percent)
  - Manufacturing
  - Insurance
  - Health Care
- Estimate of potential loss if computerized data were tampered with, erased, lost, or stolen:
  - Almost half said in excess of $5 million.
  - One quarter said between $250,000 and $1 million.
  - One quarter said less than $250,000.

Exhibit 3-3. Computer Security Institute/FBI 1996 Survey Results [5]

- Size of the damages that organizations reported:
  - Just under half (249) reported losses totaling over $100 million!
  - One quarter reported financial (institution) fraud.
  - One quarter reported telecommunications fraud.
  - One quarter reported losses from theft of proprietary information.
  - Minor losses from sabotage of data, unauthorized access by insiders, system penetrations, computer viruses, laptop computer theft, and abuses of Internet privileges.
- Over half still did not have a written policy on how to deal with intrusions.
- Most still did not have any written instructions on how to preserve evidence of tampering for legal proceedings.
- Most still did not have any “Warning” banners on their systems to indicate that they will monitor activities.
- Over half did not have an emergency response team.
- Many still did not even know if they have been attacked.
- Fear of negative publicity incurred by reporting break-ins and exposing their system weaknesses has declined somewhat.

Exhibit 3-4. Computer Security Institute/FBI 1997 Survey Results [6]

In 1996, the U.S. Senate Permanent Subcommittee on Investigations commissioned a survey in support of its hearings on *Security in Cyberspace.* WarRoom Research LLC conducted the survey of more than 500 organizations; 236 responses were summarized for the final report. This

[5] Power, Richard, “1996 CSI/FBI Computer Crime and Security Survey,” *Computer Security Issues and Trends*, Volume II, No. 2, Spring, 1997.

[6] Power, Richard, “1997 CSI/FBI Computer Crime and Security Survey,” *Computer Security Issues and Trends*, Volume III, No. 2, Spring 1997.

survey concentrated on large security organizations and on disciplines other than information security.

- 83 percent of the respondents surveyed had a security policy.
- 67 percent of respondents use a banner page.
- Over 75 percent of the respondents indicated they had a capability to detect unauthorized access.
- Over half had detected attempted intrusions.
- Over 25 percent of the respondents reported losses exceeding $500,000.

Exhibit 3-5. WarRoom Research LLC 1996 Survey Results [7]

In 1996, Datapro published the results of its Computer Security Issues review. Datapro has been conducting information security surveys since 1991. Datapro surveyed 1337 companies in several industries in all 5 major world regions. Exhibit 3-6 shows the key results of this survey.

- Concern for security has continued, but the resources devoted have hit an all-time low.
- Implementation of security strategies in practice is minimal to non-existent in many organizations.
- Most organizations have insufficient security staff.
- Only 54 percent of surveyed organizations have a security policy (down from 82 percent in 1992).
- Most organizations expressed concern about exposure to the Internet.
- Only 15 percent use encryption
- Only 28 percent have firewalls for security partitioning.
- Chief concern is that senior leaders see security as a cost that should be minimized □ they want it “invisible, invincible, and inexpensive.”

Exhibit 3-6. Datapro 1996 Survey Results [8]

Infosecurity News periodically conducts industry surveys. Its 1995 and 1997 surveys included over 1000 responses each and provide some interesting contrasts. Exhibits 3-7 and 3-8 summarize these contrasts.

[7] Gembicki, Mark, “Information Systems Security Survey,” WarRoom Research LLC, Baltimore, MD, July 18, 1996.

[8] Duncan, Rebecca A. and Jackie Hyde, “Computer Security Issues, 1996 Survey,” DATAPRO *Information Security Service,* McGraw-Hill, Camden, NJ, October 1996.

- Biggest four security-related mishaps reported were:
  - Network outages
  - Processing interruptions (denial of service)
  - Computer viruses
  - Destruction of data or records
- Lesser mishaps:
  - Theft or destruction of equipment
  - Insider computer fraud
  - Information leakage (loss of proprietary data)
  - Hacking phones/PBXs/voice-mail
  - Computer hacker break-ins

Exhibit 3-7. *Infosecurity News* 1995 Survey Results [9]

- 80 percent of the respondents perceive an improvement in security.
- 88 percent see more improvements to come in the next two years.
- 25 percent have no dedicated information security person.
- 25 percent have only one dedicated information security person.
- 20 percent see budget constraints as greatest obstacle (up from 9 percent in 1995)
- 68 percent have had a virus infection (up from 56 percent in 1995) even though 90 percent use virus detection software.
- Most common security breach was abuse of employee access privileges (40 percent).
- Nearly 75 percent have a security policy (two-thirds were updated within the last year).
- Most have a business-recovery plan and over half tested it during the last year.
- Average budget is $30,000 (up from $20,000 in 1995) with two employees.

Exhibit 3-8. *Infosecurity News* 1997 Survey Results [10]

For contrast with the U.S. surveys, a 1996 survey by the United Kingdom (UK) National Computing Centre (NCC) is presented. The NCC surveyed 9500 organizations in the UK and conducted interviews with 25 representatives from the organization to obtain additional detail. Exhibit 3-9 shows the results of this survey.

[9] *"Infosecurity News Industry Survey"* in Infosecurity News, Volume 6, Number 3, May 1995; also referenced at http://www.sevenlocks.com/scbassessingtherisks.htm, March 1997

[10] *"Infosecurity News Industry Survey"* in Infosecurity News, Volume 8, Number 3, May 1997; also at http://www.infosecnews.com/articles/9705/article2.html, May 1997

- 90 percent of the respondents had at least one significant security breach in the last 2 years.
- Average cost of the breach was over $25,000.
- Almost 20 percent of the breaches had a significant impact on the organization.
- 16 percent of the breaches caused over a week's lost time to restore operations.
- Thefts rose sharply (60 percent) from an earlier survey, with one theft exceeding $1 million.
- Many security failures involved equipment and power failures.
- Over half of the organizations were not covered with a contingency or recovery plan (reflecting the inability of the organizations to plan for integrity and availability of data).

Exhibit 3-9. UK NCC 1996 Survey Results [11]

Finally, Dan Farmer, the creator of Security Analysis Tool for Administering Networks (SATAN) conducted an informal vulnerability assessment of bank hosts connected to Internet and found that over 68 percent of those hosts were vulnerable to some form of intrusion. [12]

In general, it appears that:

- The number of computer and network incidents is growing.
- The losses associated with the incidents are rising.
- While senior management awareness of incidents and losses is growing, budgets and staffing remain relatively small.

3.3 SAIC SURVEY

To provide context for the case studies, SAIC conducted a survey of the Fortune 100 companies. Questions were oriented toward the companies' computer and network security activities, organization and staffing for information security, outsourcing practices, computer and network intrusions and incidents, motivation for information security investments, and the approach to sustain computer and network security focus and budget over time. Six companies representing a variety of industry sectors responded. The results are summarized in Exhibit 3-10.

[11] National Computing Centre Limited, "The Information Security Breaches Survey 1996," Manchester, UK.

[12] Statistics extracted from http://www.trouble.ord/survey/ (April 4, 1997).

In General:

- Policies, procedures, and standards are in place.
- Incidents are reported and dealt within a timely manner.
- Basic access controls are in place.
- Training and awareness programs, however, are limited.
- Ongoing activities cover a wide range; e.g., awareness, technology, architecture.
- Minimal amount of outsourcing - somewhat of a surprise.

Management:

- All organizations have a computer/information security department
- Most companies established the department within the last 6 years.
- Authorities of departments vary among companies.

Staffing:

- Security departments generally are led by a manager or company officer.
- Security department heads generally report through the IT chain to the CIO or CFO.
- Size is generally 10 to 40 people. All companies expect growth in staffing.

Budget:

- Three of the respondents reported growing budgets.

Intrusions and Incidents:

- Only one company said they have had no insider or outsider attack.
- One incident of a replicating file resulted in denial of service.
- Lots of virus attacks are occurring.

Business Case Models:

- Only one company uses a business case model for security investments.
- One company responded that it was not possible to develop a business case for security.

Motivation for Security Focus and Funding:

- Increased knowledge of threats.
- Corporate board and senior management direction.

Exhibit 3-10. SAIC Survey Results

The results of the SAIC survey are consistent with the other survey data with one notable exception. The staff and budgets for the security departments are on the increase, owing in a large measure, to increased awareness of the threat and actual incidents and to direction by senior management and corporate boards.

3.4 ABBREVIATED LITERATURE REVIEW

In addition to reviewing of recent survey results, SAIC conducted an abbreviated literature review of current trade publications to provide insights into parameters for the organization and business case model outlined in Section 4. Because of the common technologies, inferences about IT are assumed to be applicable to information systems technology.

Senior managers (information security and information technology) are becoming more and more aware of the need to address security and information technology investments within the context of the corporation's business goals. As Winn Schwartau has observed, "Security is no longer just about security. Today, security is about resource and information management, and it turns out that good security is a byproduct of a well-run organization." [13] He goes on to suggest that a good enterprise network security program should include the following actions: establish security goals at the highest level of your organization □ the president or the board of directors; map your networks and identify points of access, vulnerabilities, and responsibilities; perform an information asset evaluation to determine what should be protected and to what extent; institute a top-to-bottom employee education and security collaboration program; and implement the security program beginning with a solid foundation □ a sound and rational security architecture. Above all else, remember to ask the fundamental questions: "How do I know who's using my network and information resources? Do I care? Who do users claim to be, locally or remotely? Once they tell me who they are, can I make them prove it? How do I control what they do? Do I care? Do they have unlimited access to everything? Or is access restricted? And, if it is restricted, who chooses the restrictions, and how are they enforced?"[14]

Outsourcing of support services is becoming a common practice. While most companies restrict outsourcing to non-critical functions and services, information technology assets and services are becoming prime candidates for outsourcing. A recent *CIO* article also poses fundamental questions □ this time related to outsourcing: "What are your core competencies? How does your IT organization help enable corporate strategy? What IT skill sets will you need in the future? Can a vendor provide your current service levels at a lower or variable cost?" [15] The article discusses in detail a recommended process to follow once the decision to outsource has been made, but not once in seven pages of text and tables does the article address possible security concerns. In contrast, under the terms of the outsourcing agreements SEBRING negotiated, the

[13] Schwartau, Winn, "Securing the Enterprise. Technology alone won't make you safe. Tackle it as a management problem," *Network World*, January 27, 1997, page 42.

[14] Katz, Stephen, as quoted by Winn Schwartau, *ibid.*, page 48.

data center vendor "is responsible for the security of the outsourced SEBRING information technology environment, applications and for providing logical audit rights to SEBRING to test, evaluate, and report on the overall state of security by the vendor."[16] The vendor "is responsible for adhering to, and enforcing compliance by all SEBRING users with the SEBRING corporate information security policies" and "is also required to purchase dishonest employee and computer fraud insurance to cover its employees."[17]

A recent article by Miryam Williamson in *CIO* suggests an approach to setting priorities for IT projects and some criteria for IT investment decisions that are potentially applicable to information security investment decisions.[18] Exhibit 3-11 summarizes this approach.

Develop	a formal, quantitative way to assess the business value of proposed projects.
Engage	customers in a dialogue about the available resources and business needs throughout the year, not just at budget time.
Interview	customers about their wants and needs; involve them in choosing among conflicting priorities.
Communicate	frequently with customers about the Information Security (IS) department's achievements, current projects and short-term plans.
Remember	the human element. Take egos and the need for validation into account.
Work	with committees structured to minimize the influence of any one individual or department.
Visit	with the business units and ask, "How is the IS department doing?" Listen to the answers.
Communicate	clearly how priorities are set so that people can anticipate project funding decisions.
Develop	a business case for every project, assessing its risks, its business value, and the cost of building or buying it.
Demonstrate	interest in the constraints under which business customers operate.
Stay on top	of changes in the regulatory and competitive environment in which the business operates.
Be prepared	to show how a proposed project fits with business goals.

Exhibit 3-11. Approach to Setting IT Priorities[19]

[15] Field, Tom, "Caveat Emptor," *CIO*, April 1, 1997, page 58.
[16] National Communications System, *Information Security Business Case Study #1*, 25 October 1996, page 8.
[17] *Ibid.*, page 9.
[18] Williamson, Miryam, "Weighing the NO's and CON's," *CIO*, April 15, 1997, page 49.
[19] *Ibid.*, page 52.

The criteria suggested in the same article by Brian Wegner of Fortis, Inc. in Milwaukee, WI, are summarized in Exhibit 3-12. In practice, the criteria are weighted to determine a project's overall score and priority. Wegner points out, however, that he "won't put a team to work on a project that lacks a sponsor no matter how high its score in other areas." [20]

Business Strategy:	How well does the proposed project fit with the company's overall business strategy?
Return on Investment (ROI):	What is the anticipated ROI?
Ability to Deliver:	What is the likelihood that the IS department will be able to fulfill the project requirements within a reasonable time?
Business Readiness:	Is the business equipped to adjust to the changes the new system will demand?
Regulatory or Mandated Changes:	Is the proposed required because of some change in the business environment?
Business Values:	Is the change in harmony with the corporate value system?
Cost Assessment:	What is the best estimate of the project's cost?

Exhibit 3-12. Criteria of IT Investment Decisions [21]

An example of the regulatory or mandated changes in criteria shown above is found in a recent article about the security implications of the Telecommunications Act of 1996. "Officials at the Federal Communications Commission (FCC)are eyeing plans to protect the phone companies' phone switches with vast quantities of new information-security gear. The effort, which would be funded by customers' monthly charges, is needed because the phone companies are required by 1996 telecommunications reform law to share their networks." [22] Funding on a shared public/private-sector basis could also be mandated by the FCC.

Some people are saying "finally, it's starting to happen: IS and business goals are converging." [23] Can the convergence of information security and business goals be far behind? Heath Row summarizes the eighth annual *CIO*/Ernest & Young survey of 230 CIOs, their bosses, and their peers. IS and business goals are becoming more closely aligned. "CIOs and business executives are both looking at IT not just as a cost center but as a strategic tool, and IS leaders are increasingly accepted as business partners by their bosses and peers." [24] The article points out that

[20] Wegner, Brian, as quoted by Miryam Williamson, *ibid.*, page 53.

[21] *Ibid.*

[22] Capital Roundup, "Network Security," *Washington Technology*, May 22, 1997.

[23] Row, Heath, "Taking Care of Business," *CIO*, April 1, 1997, page 63.

[24] *Ibid.*

CIOs, bosses, and peers view aligning IS and corporate goals as the CIO's top priority. The article also points out that "The differences in present and future priorities of the CIO suggest that emphasis on operational optimization will decrease and emphasis on value creation will increase."

Finally, according to a recent *Information Week* article, " A new way to think about IT's return on investment is taking hold." [25] In short, this new way of thinking includes intangibles (those things the customers really care about) in the ROI equation. Examples include product quality, customer satisfaction, time to market, when to invest in technology, and shareholder value. Proponents such as Erik Brynjolfsson at the MIT Sloan School of Business and Robert Benson, a professor of information management at Washington University in St. Louis, suggest that the new way of thinking has emerged in part because of the heretofore inability to measure the benefits of information technology adequately. The article goes on to suggest that risk analysis and economic value added are two additional approaches being used to establish ROI. In practice, most companies are using a mixture of approaches □ some old, some new. As an indication of the growing interest, *Information Week* has added a regular feature on return on investment (ROI).

While admittedly brief, the literature review does suggest that companies are:

- Taking a broader look at security □ it is not just technology.
- More frequently making information technology investments in the context of the business goals.
- Looking for, and in some cases practicing, new methods and measures of determining return on investment that take into account intangible factors.

3.5 ATKINSON SECURITY PROJECT

In 1989, the American Society for Industrial Security (ASIS) sponsored a research project at the Wharton School of Management at the University of Pennsylvania to study the best approach to

[25] Violino, Bob, "Return on Investment," *Information Week*, June 30, 1997, page 36.

implementing security management.[26] This endeavor was named the Atkinson Project in honor of James Atkinson of Johnson and Johnson. Mr. Atkinson was a long-term leader and advocate of value-added strategies in security management. The goal of the project was to “realign security management techniques from a *cost center* approach to a *profit center* approach based on the development of a methodology for assessing the value-added of investments in security projects.”[27] The project identified three different approaches to modeling security management: the cost-center approach; the profit-center approach, and the consulting approach (a middle-of-the-road approach). All three models or approaches can implement from one to all aspects of a viable security program. The major differences among them are: orientations on the corporate objective(s); emphasis on building the stockholders’ wealth through contribution to equity; and the consequences of investment in security tools and methods.

To understand the underlying differences in approach, the consequences of viewing a function as a cost center or as a profit center must be clear. A cost center is any accounting unit of a company or corporation that incurs costs without making any substantial contribution to shareholders’ equity; while it might appear that this situation is totally undesirable and should be eliminated, there are many fact-of-life expenses in running a business owing to personnel, regulation, and other requirements. A profit center on the other hand, also incurs some expenses as a routine of doing business, but it also brings a return on its investments □ ideally a substantially high positive number in the algebraic balance.

In classical accounting, there are several methods that may be used to measure this return on investment. Circumstances will prescribe which one to use. A critical insight is the necessity for viewing any and all organizations and functions in their true role as profit centers if that assessment is appropriate. The most important reason for viewing an organization as a profit center is that this proper assignment will affect □ drastically □ the types and factors of investment decisions made by their managers. For the security manager, especially at the divisional or

[26] Duncan, Keith, Stephen Gale, John Tofflemire, and Rudolph Yaksick, “The Atkinson Security Project,” A Special Issue of *Security Journal*, Volume 3, January 1992.
[27] *Ibid., page 2.*

corporate level, these decisions can be quite weighty in leveraging the use of corporate funds to maximize shareholder equity.

The main reason for this concern about accounting methods is the realization that most companies and corporations treat security as a cost center. In the corporate budgeting cycle, the security manager is usually given a funding allocation judged to be adequate to get the security job done to some minimally acceptable standard. This loose measure of effectiveness (MOE) is set by a senior executive who often may not appreciate how investment and ROI can possibly apply to security. As a result, the minimal investment results in staff members doing a merely adequate job that demands little accountability for increasing the shareholders' wealth.

Now, consider that same security function treated as a profit center. In the profit center all investments are assessed in terms of their possible ROI, using the most appropriate measure. In terms of security, management can employ a number of different ways to secure a facility and prevent losses. To judge the most effective ROI for each of them, the security manager determines as accurately as possible the baseline of losses from the cost center method used in the past, at comparable corporate facilities, or from industry experience. The security manager then calculates the expected losses of each of the varied methods of security, expressed in terms of dollars of equity or revenue lost. The net gain or loss from the baseline case can be taken as the overall ROI against the cost of the method.

As an example, a given warehouse may have a consistent record of inventory shrinkage over a reasonable baseline of time. Several methods of increasing the security of the facility might be considered, including an increased security guard force, different procedures and methods to check entering and departing personnel, magnetic tags on high-value assets, and surveillance cameras and other expensive electronic devices. To measure their effectiveness and assess their cost of operation, the actual procurement costs, industry experience with the probability of cost reduction, and the actual value of the inventory warehoused can be used to calculate the expected value in terms of ROI, using the net present value (NPV) method of determining the amortized cost and values involved, the internal rate of return (IRR), or the cost-benefit analysis (CBA) method.

The project report includes the Atkinson Model, a security investment decision-making mathematical model. The model has not been widely applied because of difficulties in measuring the ROI. With the advances being made in including intangibles (including the security motivations highlighted above and in following sections) in the ROI determination, the Atkinson model may possibly now support business case determinations.

3.6 OBSERVATIONS AND CONCLUSIONS

Security incidents and reporting alone are not sufficient to maintain a strong focus on security. The most effective motivation for security focus and funding is provided by senior management with the attention of the corporate board. This appears to be consistent with the Case Study results and conclusions. Although corporate regulatory audit and management oversight generates the most significant justification for information security programs, it offers little insights into information security business planning and integration.

The growing convergence and alignment of information systems and business goals portends a favorable environment for convergence and alignment of information security and business goals.

Use of business case models for information security investments is minimal. This appears to be consistent with the Case Study results and conclusions.

The growing acceptance of using intangibles and other approaches in determining return on investment suggests a more favorable climate in the future for security investments, since intangibles represent a significant motivation for those investments.

SECTION 4
ORGANIZATION AND BUSINESS CASE MODEL FOR INFORMATION SECURITY

Section 4.1 summarizes what was learned from the four individual business case studies and from an analysis of the literature. It represents a collective view that incorporates the unique experiences of each organization's previous information security measures, incident/accident mitigation, lessons learned, risks, and costs.

Section 4.2 describes the organization and business case model for information security. The features are representative of each organization that was reviewed. It shows the abstracted information security investment decision and procedural flows.

4.1 WHAT WE'VE LEARNED

As indicated in the introduction, information and telecommunications technology and services have expanded business functionality at an astonishing rate. In the face of rapid technological, regulatory and societal change, many organizations have undergone significant changes in the way they conduct their business activities and in the way they view information security. Each of the four participants in the case studies recognized increased risk to their business operations over the last few years and responded accordingly. Some of the lessons learned from those responses include the following factors, which are included in the organization and business case model.

4.1.1 Network Intrusions

The case studies showed that while single, highly visible incidents of network intrusions or security incidents sparked added investments in security programs, they do not provide the focus and motivation needed for long-term solutions. Research indicated that when incidents were the primary motivation for security funding, management interest, monetary allocations, and security program effectiveness followed a bell curve pattern. The organization with a small security program would experience a significant security incident and allocate extensive follow-on funding to address the issue. Once the incident was corrected, the funding would taper off, leaving the organization exposed to another significant incident. Successful programs are funded at a consistent and adequate level to ensure risk exposure is minimized. Over time, the bell curve approach not only offers a level of protection insufficient to counter the security risks, but also is much more expensive than the consistent or straight-line approach to security funding.

4.1.2 Costs of Network Intrusions/Security Incidents and Costs of Recovery

In general, companies do not capture the costs of recovering from network intrusions and other security incidents. The primary motivation for doing so would be to establish dollar value of loss in order to charge and prosecute the perpetrator. The case studies and other evidence suggest that companies are reluctant to pursue civil or criminal remedies because doing so might expose vulnerabilities and possible malfeasance to the general public.

4.1.3 Deter-Protect-Detect-Contain Capability

The SCOUT case study clearly showed the wisdom of proactively establishing a capability to deter network intrusions and security incidents, protect network and other information technology assets adequately, detect intrusions and other security incidents, and contain network intrusions and security incidents if and when they occur. While detailed cost savings were not collected or projected for the two security incidents addressed by SCOUT's PSP and reviewed in the detailed case study, it was obvious that lost revenue alone would have been significant had the program not been in place.

4.1.4 Legal/Regulatory Oversight

While all of the participants linked their information security programs to codes of business conduct, two out of the four business case participants also informally linked their programs to the Federal Sentencing Guidelines Compliance program. Although not specifically addressed yet by the industry baseline benchmarking referenced in the Guidelines, as the revised recommendations of the U.S. Sentencing Commission are implemented to address computer fraud and abuse violations of U.S. Code, the benchmarking probably will be expanded to address this important area. The impact of such an event will further support increased emphasis and justifications for security. (See Appendix A for a discussion of the changing guidelines.)

For example, AMBASSADOR periodically includes computer security issues within the Code of Business Integrity program and integrates its results with the Federal Sentencing Guidelines Compliance Program. AMBASSADOR is thereby sending an important message to its employees to act within the highest ethical and legal standards. That behavioral reinforcement is of critical importance in today's information age, where virtually every business communication moves over at least one "position of trust" link of the public switched network infrastructure. AMBASSADOR is also extremely forward-looking in its support of the Federal Sentencing Guidelines, which recently added language to address violations of the federal computer crime statutes and recent amendments to those statutes.

In all four case studies, the impact of regulatory oversight and deregulation was a significant information security factor. Each of the three telecommunications companies in the study felt compelled to understand and address the security issues related to open network architecture, unbundling, co-location, mandated interconnection of operations, signaling and operator services systems. Two of the three telecommunications companies had to explain to their boards of directors the implications of and strategies needed to address recent significant intrusions into their information technology operations. Each of the three was involved actively in addressing the security implications of the Telecommunications Act of 1996 with federal and state regulators and industry advisory councils like the FCC's Network Reliability and Interoperability Council

(NRIC). One of the four case study participants had to appear before Congress to explain its perceived failure to adequately address information security and critical systems integrity.

4.1.5 Growing Dependence on Distributed, Highly Networked Information Technology

This issue was best captured by three of the four case study participants, those who have recently gone to the corporate board or other oversight body concerning information security and denial-of-service (service outages) exposures and liabilities.

In 1987, a high-visibility incident occurred at EL DORADO in which mission-critical flight software was found to contain several unauthorized changes. Before the return to flight operations, the agency conducted a six-month independent security review. The independent review found that EL DORADO systems were vulnerable in several areas, including access control, management control, and disaster recovery. Overall, the review team identified approximately 80 specific items that needed technical or management attention. In response to the findings, EL DORADO management formed a diverse security team to address the problems in all specific systems and to initiate an action plan that would address the security concerns for all systems throughout the center.

The senior management teams at SEBRING, SCOUT, and AMBASSADOR each recognized that their networks were not as secure as they would like them to be. Before the intrusion or outage, their security concerns were general in nature. Internet connectivity started as a technical whim and grew very fast. Management failed to recognize and take control of the technology as it was planned, engineered, and inserted into the operations environment. People and business units were connecting to the Internet on their own, thereby introducing new risks and exposing the PSN operations backbone network. Personnel need to be reminded of the security exposures and the security policies that justify the centralized control and the attendant procedures and processes. Centralized control of what was bought and connected to or put on the network/desktop became a tactical objective of the newly created information security team.

A denial of service attack (DOS) [28] against SCOUT's Internet Service Provider (ISP) subsidiary caused the loss of an Internet service component to the public. The attack was immediately detected when the loss of service occurred. The economic losses resulting from the three-day incident exceeded $20,000 in lost services and additional labor costs to detect, isolate, investigate, and mitigate the intrusion. Had SCOUT not had the interdepartmental 24 hours a day, 7 days a week reporting, incident response, and investigation capability in place, the impact could have quickly spread to other SCOUT ISP services and servers in a fashion similar to the denial of service losses experienced by other ISPs. [29]

The security program within AMBASSADOR developed significantly in both scope and depth by two compelling IT related events. The first event was a postmortem of a major outage of the PSN in the early 1990s. Although it was later determined that the outage was not caused by a security incident, the investigation team found software security and change control to be seriously deficient within the affected signaling network elements. Deficiencies in separation of responsibilities, least privilege, and audit logging were also cited and addressed during the investigation. A second, more recent, compelling event supporting the security program within AMBASSADOR involved the findings of an internal audit of contingency planning for a work stoppage. The risk analysis conducted as part of that contingency planning audit effort determined that network elements of AMBASSADOR's PSN were at considerable risk from potentially disgruntled technicians. The analysis also found that AMBASSADOR was dependent upon remote PSN operations, administration, maintenance and provisioning (OAM&P) systems networking and personnel that could be exploited if additional physical and logical access controls and countermeasures were not put into place.

[28] The incident involved an attack technique known as a TCP SYN attack, in which a perpetrator's host transmits a large volume of connection requests that cannot be completed because the intended addresses for the connections are bogus. This quickly caused the connection queues of the ISP server, in this case the targeted component server, to overflow denying service to legitimate customers for more than 3 days.

[29] In early September 1996, an unknown criminal hacker attacking the PANIX Internet Service Provider in New York City used a similar TCP/SYN-flooding attack. This attack denied service to legitimate users and forced the ISP to take its servers out of service for an extended period until software patches to alleviate the attack had been installed. Identical attacks have incapacitated several other service providers in the past few months.

4.1.6 Customer/Marketplace Expectations

While security has never been easy to justify, absent the personal corporate experience of a major highly visible security incident, the business case studies found that the demands and expectations of IT networking customers and the marketplace are beginning to send a more ominous and strategic message on information security and availability. Customer confidence and trust in the integrity, security, and reliability of AMBASSADOR’s PSN service offerings and internal systems supporting the PSN are the number one business driver for AMBASSADOR’s security program. This level of commitment to security, coupled with increased customer and regulatory interests in the security of the PSN, have caused AMBASSADOR’s audit and compliance programs to take an expanded look at computer and network security regularly.

4.1.7 Other Motivations

Shareholder/Stakeholder Value - The primary goal of every public company is to maximize shareholder value and ensure the continued viability of the company. Security incidents, especially if they receive coverage in the press, can have negative effects on share valuation.

Capital Market Perception - Growth (and survival) of the company is dependent on capital and the source of the capital is the capital market. The perception the capital market has of the company is critical to the continued success of the company.

Securities Rules and Regulatory Compliance - These additional regulations influence the manner in which trading of the public company’s stock will take place, affecting the ability of the company to raise capital through public stock offerings, etc.

Assurance/Insurance - Every business must be concerned about assurance (continuity) of its business operations and what insurance investments may be required for that assurance. Information security is a vital ingredient of business assurance. For insurance, difficulty in determining the value of information has deterred insurance offerings for information security.

The only exception to this is the limited insurance coverage available for websites based upon the National Computer Security Association’s Web Certification Program.

Competitive Advantage - This motivation can be a two-edged sword. Information security investments may be considered a cost burden in a highly competitive environment. On the other hand, these investments have the potential to improve service availability, privacy, and integrity in the face of a growing threat.

Media - Like competitive advantage, media attention can be viewed as negative or positive. Favorable attention creates a competitive advantage and vice versa.

Intangibles - There are many tangible and intangible costs and benefit considerations that serve as motivation for security investments. Exhibit 4-1 lists some of these considerations.

Avoid Costs		**Increase Benefits**	
Tangible	**Intangible**	**Tangible**	**Intangible**
▪ Potential Regulation and Litigation (Civil and Criminal) ▪ Liability ▪ Loss of Human Life ▪ Proprietary Information Loss ▪ System Down Time ▪ Lost Business ▪ Inability to Field New System(s)	▪ Shareholder Confidence ▪ Public Perception and Trust ▪ Market Share ▪ Congressional Oversight ▪ Perception of Liability ▪ (Corporate Officers’ Fiduciary Responsibility) ▪ Vender Performance History	▪ New or Renewed Contracts ▪ Ability to Mitigate Security Incidents ▪ Federal Sentencing Guidelines Compliance	▪ Meeting New Needs of Business ▪ Satisfy Needs of Regulators ▪ Satisfy Needs of Shareholders ▪ Satisfy Public Opinion ▪ Exceed Customer Expectations

Exhibit 4-1. Intangible Motivations

4.2 THE MODEL

4.2.1 Introduction to the Model

The hypothesis of this effort was that the cost of reacting to intrusions is greater than preparing for them by establishing a security program in advance. While the hypothesis was not disproven, there was insufficient cost data available to substantiate it. However, during the analysis of the observations, results, and conclusions of the four case studies and the supplemental research, two prevalent themes emerged. Organizations react to a variety of motivations for security investments, not just return on investment; and significant security investments (generally over $1 million dollars) are subject to the rigors of a business case justification □ as are all other significant investments. In the absence of a single network intrusion or security incident that might provide motivation for security investments, the following model for information security investments is proposed. The model takes into account and is organized about the two prevalent themes.

The organizational model will be discussed in terms of an ideal organizational climate from the standpoint of information security and in terms of the structure and process used to determine and approve security investments. The business case model will be discussed from the standpoint of traditional models with a view toward incorporating emerging concepts.

4.2.2 The Organizational Model

As suggested by the ESCORT organization in Exhibit 2-2, which captures the best of the case studies, and by the research, the ideal organizational climate from a security standpoint includes a simple statement of corporate security policy that is endorsed by the CEO and is widely disseminated and incorporated into the standards of conduct for employees. The policy clearly identifies responsibilities and accountability and the consequences of failing to follow the policy. The policy is updated frequently to incorporate changing business and technical environments. A mechanism for enforcing the policy is in place, used, and checked.

The senior management of the organization is concerned about the entire security equation, not just the technical aspects. Security goals are established as a part of the vision and strategy for the corporation. Senior managers view the company as being vulnerable and visibly insist on accountability for security. They understand that the security posture of a company is very dynamic. When implemented, changes in business practices and technology, introduction of new applications, mergers and acquisitions, similar incidents invalidate the perceived security posture.

Business cases for all investments fully address security implications and costs. A detailed review of the security posture is conducted annually.

Metrics on security are established and regularly analyzed. These metrics include the number, nature, impact, and time to resolve intrusions and other security incidents. These metrics address physical and electronic incidents and incorporate related activities such as asset management.

The security department is staffed based on the business environment, stability of the company, the information technology environment, and the perceived risk. Proper staffing is determined by benchmarking, audits, risk analysis, and the like. In the event the security expertise is distributed throughout the company, adequate procedures and communications mechanisms are in place to coordinate responses to security incidents rapidly and to bring the appropriate expertise (no matter where it is located in the company) to bear on the incident. The head of the security department is a manager and/or a company officer who is knowledgeable of and focused on the business goals of the company.

While the placement of the department within the organization might vary, the department head has frequent access to the Executive Council (e.g., President, COO, CFO, CIO) of the company. In addition, periodic reports on the security posture of the company are provided to the Corporate Board or an appropriate committee of the Board.

Formal and informal lines of communication should exist between the security department and the business units. These lines of communication are used frequently to establish and satisfy needs for security capabilities, to provide technical advice and assistance, to train, to send and receive threat information, to report and disseminate information relating to network intrusions and security incidents, and to coordinate the responses to those intrusions and incidents. These lines of communication are linked at appropriate points with the operations centers of the business units.

A special relationship exits between the Chief Information Officer and the head of security. While it may be a senior-subordinate relationship, it is based on a mutual understanding of the company's information technology environment. Together, they pursue the convergence of the business, information services, and information security goals of the company. They receive the support of the business units and senior management in articulating the value added by information technology and security to the Executive Council. They work together to ensure there are no surprises to the Executive Council. In coordination with the business units, they have established integrated business assurance plans that are coordinated with legal, public relations, and other key departments. They have collectively established capabilities to protect the corporate information infrastructure from physical and electronic threats, to detect intrusions and other security incidents, to contain the effects of intrusions and incidents, and to deter threats.

By way of background, each organization structure differs in details; and each responds to their market and operating environments which overlap but are quite different. The inclusion of the government organization with the three commercial sector organizations should be viewed as providing depth and breadth to the business case database and not as a source of inconsistencies.

Exhibit 4-2 shows the organizational security strategy model. To some extent, the four case study organizations provide statistical representation across widely varying purposes, markets, and size.

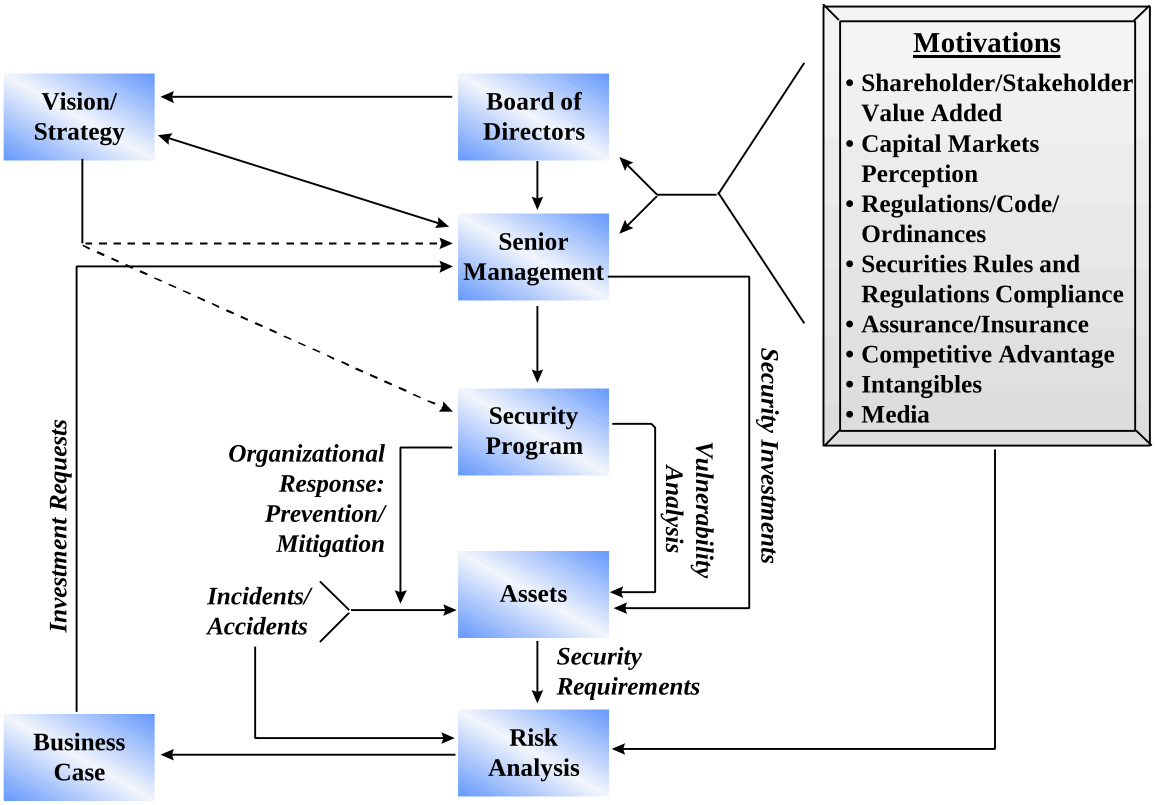


Exhibit 4-2. The Organizational Model

The board of directors has overall responsibility to the stakeholders. The directors are responsible for the general ability of the organization to achieve its business purposes and objectives. In collaboration with senior management, the board establishes the overall vision and business strategy, which establish the overall focus of the organization. On behalf of the stakeholders, they look for a growth in added value and corporate wealth (increased return on capital investment, increased market share, increased dividends/stock price).

Senior management, the managers of the business units, the CIO and security manager, and the heads of other departments implement the policy and decisions of the Corporate Board and senior management, report on operations, and make known the investment needs of the company. From a security standpoint, they are the policy implementation and execution portion of the organization and are collectively responsible for the security posture of the organization.

By way of example, the vision and strategy of each private-sector case study organization varied from the relatively simple and succinct (e.g., "build the best product …" or "provide the most reliable delivered services …") to the more involved and detailed. Each statement implied the need for security (information security, physical security of facilities, and the health and safety of personnel). Two of the case study organizations defined these needs in terms of organizational entities (e.g., department or division), which have explicit and primary responsibility for ensuring day-to-day security of the organization's processes (generally proprietary in nature) and the "information security" of its products and services. Other organizational entities, such as legal, management audit, corporate audit committee, and finance have secondary, but defined, responsibilities to ensure that the organization with the primary responsibility can carry out its functions. This represents the explicit devolution of ensuring "information security" tasks and activities are carried downward and laterally throughout the organization.

The actual information security program, both prevention and mitigation, is defined in detail in the organization's policies, procedures, and manuals, as well as related information security bulletins and organizational newsletters. The organizational entity at this level is the first and principal level of response team to an information security incident or accident. As such, it will apply appropriate measures of mitigation to minimize "the risk to the organization." Through vulnerability analysis, it will identify both preventive and mitigation investment strategy alternatives. Specific risk analysis will assess the potential risk impacts (that is, in costs, loss of revenues, customer dissatisfaction, etc.) on the assets of the organization (organization value, physical plant or facilities, personnel, environment, customer base or market share, information systems hardware/software, services, etc.). The risk analysis identifies the high-risk, high-cost, low-tolerance thresholds for information security prevention and mitigation investment strategies. The risk analysis also addresses organizational procedures and identifies and defines these for incorporation into the organization's policies and manuals.

The entire organization is motivated to act in certain ways by a variety of influences. People and sub-organizations principally respond to the external environment influences which affect the wealth of the organization and the stakeholder. The box labeled "motivations" captures the principal stimuli of the business environment that the organization responds to and, depending on organizational purposes, may try to influence its business objectives. Principal among these is the value added to the stakeholder (or shareholder). Stakeholders require some contingencies in added value directly related to their level of investment (psychic as well as monetary). These stakeholders include individual and/or organizations seeking constructive returns on their investments as well as senior management, business managers, and department heads. In the private sector organizations, stakeholders include stockholders (and bond holders), but also regulators for public purposes and the securities industry which supports the growth and self-regulation of business. Stakeholders also include competitors. In public organizations, the stakeholders include other portions of the same department or agencies, other agencies, the Congress and President, and even in some instances foreign entities. Each of these entities influences, directly or indirectly, the information security risk and risk tolerance of the organization.

4.2.3 The Business Case Model

Business case methodologies and techniques have demonstrated their usefulness in our understanding of how organizations make investment decisions. The methodologies generally include the following steps:

- Identify the decision criteria (i.e., investment/financial/economic as well as technical, operational, and market)
- Develop the key success factors.
- Establish a baseline against which alternative investment strategies can be evaluated and their risk(s), effectiveness, and efficiency assessed.
- Evaluate alternative ways of improving overall organizational and procedural effectiveness and efficiency (i.e., maximizing value added to the stakeholders).

Interviews and analyses of four different organizations (one public and three private-sector) whose businesses are heavily influenced by and dependent upon information security demonstrate that the business case approach is useful in determining how information security investment decisions are made and implemented. SAIC used the above considerations to develop a generic information security business case model and suggest how the decision process might be modified to emphasize information security and its potential contribution to enhance value added to the organization.

Several different types of business case models could be used to describe and abstract the individual cases. These business case model approaches include:

- Economic/Financial/Accounting/Process
- Impact (Risk versus Cost)
- Delphi Technique (Consensus)
- Survey and Market
- Focused Interviews
- Composite
- Broad/Interactive
- In-depth (Vertical Bore/Focused Topics).

The derived model is a composite framework that can incorporate the principal features of each of these, particularly the financial, economic, and accounting tasks. This incorporation permits the information security investment analyst and planners to address questions and investment alternatives in depth and breadth consistent with the range and depth of the data. It also allows for ease of extraction, assessment, and allocation of common results from among the individual case studies.

These case study organizations have in common information security programs in place that encompass both prevention and mitigation actions. These programs have evolved based on “business risks” and experience. Each organization has experienced various information security incidents and/or accidents that affected or potentially affected the ability of the organization to fulfill its business purposes and functions. Each organization responded to each incident/ accident by taking direct action in the form of investment decisions and modification of either or both its organization and its procedures. The range of responses was proactive as well as reactive.

The derived business case model is similar to and mappable to the Atkinson Model introduced above. This model, however, is more representative of the organizations reviewed in this case study. It is sufficiently flexible to incorporate the range of methodologies, technologies, procedures, and the decision/implementation (execution) processes that were used by the interviewed organizations. It captures the flow of the decision for investment in and implementation of each information security strategy.

There are two formats for the business case. The two formats vary significantly in detailing the organization's capital budget process and cycle □ both approved and proposed budgets.

The signature authority is established by corporate policy and procedure, and may require the signatures of the COO and the chairman of the investment committee. The signature authority establishes the organizational signoff and approval to commit and expend investment and operating funds. Generally, specific thresholds are set for each organizational level. The $1 million and greater threshold often requires the signature of the CEO, COO, and CFO. It will generally have a "recommendation" signature from the CIO and executing security officer or manager. It is not uncommon to require a signature also from the board of directors, usually the chair of the investment committee, particularly if the threshold is exceeded significantly.

Information security capital (and related operations) investments that exceed the $1 million threshold often are considered strategic in nature because they usually represent investment expenditures over more than 1 year and generally have a wider and more pervasive impact on the organization. This threshold and "strategic" perspective differs from many other organizations that generally use a more traditional 5-year horizon. Information security technologies evolve rapidly and as a result, their effective useful life span is significantly shorter corresponding to the need to upgrade frequently or replace them with more current technologies. Thus, the strategic time horizon for information security is as short as 1 year.

Exhibit 4-3 shows the formal business case outline that is used to request and approve funds for information security capital investment funds.

- Executive Summary
- Project Description and Objective
- Opportunity Section
  - Market Opportunity/Ensure Stakeholder Value
    - Products and Services
    - Competitive Thrust/Advantages
    - Benefits - tangible and intangible
    - Revenue Protection/Growth
  - Process Improvement (Security Prevention and Mitigation: Near-Term and Long-Term)
  - Legal (Mandatory) Requirements/Compliance
- Alternatives Evaluated (Investment Strategies: Near-Term and Long-Term)
- Analysis, Alternatives Ranking, and Recommendation
  - Data Collection and Analysis
    - Capital Requirements
    - Expense Requirements
    - Quantification of Savings/Cost Avoidance
    - Demand Forecast
    - Revenue Forecast (Near-Term and Long-Term)
  - Financial Analysis (Security Analogies Must be Specific)
    - Basics Assumption Cashflow, Benefits, Disposal Costs
    - Net Present Value/Internal Rate of Return/Benefit-Cost Ratio
    - Discounted Pay-back Period
    - Modified Profitability Index
    - Economic Contribution (to Company Value)
    - Capital and Expense Utilization
  - Project Analysis
    - Risk/Sensitivity
    - Technology
    - Operations/Implementation
    - Marketing
    - Impact on Other Products/Projects (Near-Term and Long-Term)
    - Intangibles
    - Strategic Fit
  - Ranking of Alternatives
  - Recommendation
- Implementation (Near-Term and Long-Term)
    - Work Plan/Timeline
    - Marketing and Communication
    - Technology and Core Operations
    - Support Functions
    - Legal and Tax Issues
  - Project Inter-dependencies
- Financial Summary
- Performance Measures and Measurement
  - During Implementation
    - Capital
    - Revenue
    - Expenses
  - Post Implementation
    - Capital
    - Revenue
    - Expenses
    - Market Penetration
    - Market Share
    - Customer Satisfaction
    - Savings
- Appendices

Exhibit 4-3. The Business Case Model

Most organizations, particularly those with large revenues (sometimes exceeding $2 billion or more in gross revenues), require that this outline be completed before any capital investment can be approved and funded. The outline is designed to address broad business questions rigorously in order to ensure that competing alternatives (including information security) are evaluated and compared against the same performance measures or actions. Senior management, with the board of directors, can then assess the ability of each investment alternative to "deliver the projected performance" and the likelihood of benefiting from or contributing to the cross-impact with other investments. Documents are generally 10 to 20 pages in size and may contain appendices that provide supporting data and analyses. These decisions are designed to improve decision quality and lead to increased stakeholder value; invest in major hardware and software investment resulting in productivity improvements; enhance competitive advantage; and enhance or acquire market share.

The next threshold consists of those capital investments that exceed $500,000 and are less than $1 million dollars. Signature authority at this level is usually limited to the heads of business units or large operations functions in the organization. Frequently, the approval signature of a financial officer of the organization is also required. Two of the three commercial organizations required a shorter decision support document. Exhibit 4-4 is an outline of the content of this document that is required at this signature authority level.

- Title
- Objective and Description
- Alternatives
- Analysis, Conclusions, and Recommendations
- Implementation Schedule
- Interfaces, Policies, Procedures, Sign-off, Concurrences
- Attachments

Exhibit 4-4. Decision Support/Document Outline

This document is considerably less comprehensive, and more tactical in focus (i.e., generally 1 year or less), and has a less pervasive impact on the organization. Its focus is on why the organization needs the investment and why they need to make the investment at this time.
This level of format is useful to respond immediately to requirements generated by current or eminent information accidents/incidents. At this level, it is not unusual for collective decisions to be made by no more than 2 to 4 decisionmakers. The risk levels and tolerances can be assessed quickly and the organization is able to respond quickly to immediate accidents and incidents requiring decisions and actions.

The lowest signature authority threshold is generally restricted to selected operations managers and directors. The thresholds are capital or new operating investments greater than $100,000 but less than $500,000. Its horizon is anywhere from a few days to less than 1 year. It focuses on current problems that require immediate resolution or prevention. It is not uncommon for action to be initiated before receiving completed organizational approval.

The latter two signature authority levels focus on hardware, software, and service investments that maintain and preserve the existing systems (including minor improvement), i.e., those items that are "critical to the continuity of the business."

The range and size of prevention and mitigation capital investment requests from a significant piece of information that represents a "pulse" of the organization's internal operating environment. When this information is coupled with the motivations resulting from the stimuli of the external operating environment, senior management, in concert with the board of directors, has the significant information necessary to review and revise the corporate vision and strategy annually. This timing and the "collection of information" for the decisionmakers present a regular opportunity for the organization to reassess its risk level preferences and tolerances to information security accidents and incidents. As pointed out in a recent issue of the Harvard Business Review [30], all good business cases include four key elements: the people or team, the opportunity or

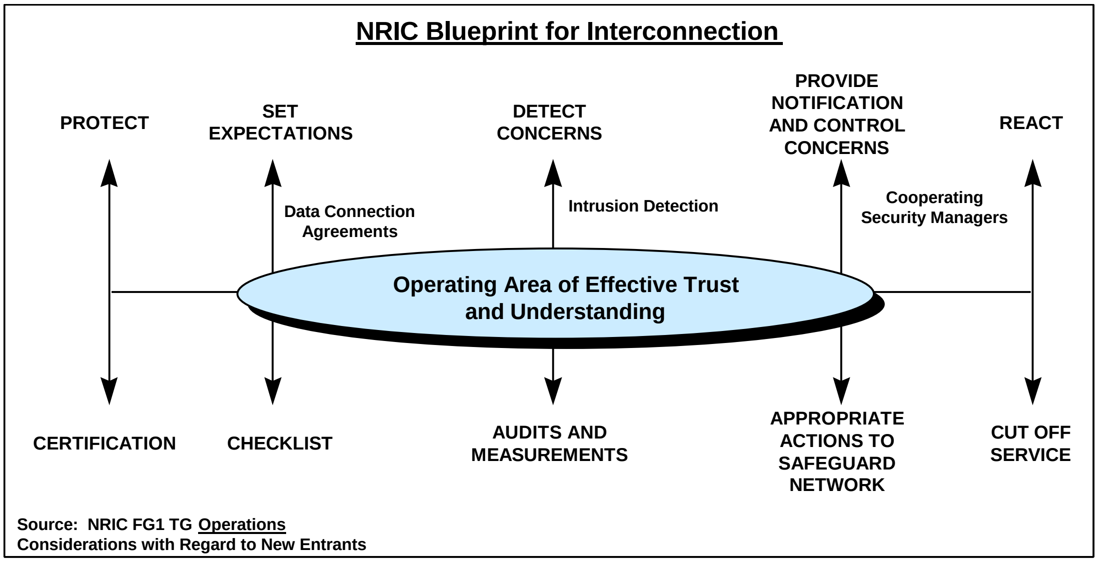
[30] Harvard Business Review, July- August 1997, *How To Write A Great Business Plan*, page 98.

problem to be addressed, the context (big picture/regulatory environment), plus risk and reward assessments.

SECTION 5
SUMMARY

5.1 GENERAL

Each case-study participant recognized increased risk to the information technology supporting their critical business operations over the last few years owing to a variety of factors. While all of the participants linked their information security programs to codes of business conduct, two of the business case participants also informally linked their information security compliance programs to developing legal obligations incorporated within the Federal Sentencing Guidelines. The impact of regulatory oversight and deregulation was a significant information security factor in all four case studies. Each of the three telecommunications companies felt compelled to understand and address the security issues related to de-regulation brought about by the Telecommunications Act of 1996. All three also supported the concepts and recommendations of the Network Reliability and Interoperability Council (NRIC) to address such open market issues within an area of effective trust and understanding. Exhibit 5-1 shows the NRIC approach to the security issue.


NRIC Blueprint for Interconnection
PROTECT
SET EXPECTATIONS
DETECT CONCERNS
PROVIDE NOTIFICATION AND CONTROL CONCERNS
REACT
Data Connection Agreements
Intrusion Detection
Cooperating Security Managers
Operating Area of Effective Trust and Understanding
CERTIFICATION
CHECKLIST
AUDITS AND MEASUREMENTS
APPROPRIATE ACTIONS TO SAFEGUARD NETWORK
CUT OFF SERVICE

Source: NRIC FG1 TG Operations Considerations with Regard to New Entrants

Exhibit 5-1. Approach to Telecommunications Deregulation Security Issues

While there are important insights and compelling stories for information security contained within each of the four case studies, the common theme apparent throughout is the necessity for information security programs to be lean, mean, proactive, focused, and aligned to the business mission. If information security is to be dynamic and longstanding in its mission, then it must be justified along the lines of other business cases and functions. While not an exact science, information security is developing with respect to its contribution to the business mission, bottom line, and strategic focus of enlightened companies and entities.

5.2 LESSONS LEARNED

Getting companies to agree to participate in the case studies was very difficult. It was found that a trusted, personal relationship was required even for initial access to information about companies which might suggest their participation.

The goal was to include in the case studies those companies that had a significant network intrusion. Several companies were identified as very promising candidates as case studies, but they would not participate because of counsel by the company's legal department or because of ongoing or contemplated prosecutions of intrusions.

Quantification of justification for security investments is very difficult. Threat data is generally vague and, except for investigations by the FBI or prosecutions by U.S. Attorneys, it is not aggregated across companies. Cost data on network intrusions and internal incidents are generally not captured and when they are, the data are not of sufficient detail to support business case analyses. [31]

[31] Indeed, Don Ingraham, the renowned prosecutor from Alameda County, CA, has found that the number one case for the loss of computer-related crime cases is the inability of victims to document and support their losses or damages.

5.3 SUGGESTED FUTURE EFFORTS

Encourage the National Security Telecommunications Advisory Committee's (NSTAC) Network Security Information Exchange (NSIE) to become involved. Offer the results of this effort to the NSIE for use by the member companies and request participation by the member companies as case studies to expand these initial results.

Explore the possibility of including new approaches to return on investment and the use of the Atkinson Model for justifying security investments in the business case model presented. This should be done with proponents in the academic community and with companies practicing some of these new approaches.

Explore risk management techniques and tools for possible application and inclusion in the business case.

APPENDIX A

ANALYSIS OF THE IMPACT OF U.S. SENTENCING GUIDELINES ON INFORMATION SECURITY

The attached copyrighted paper is reprinted with permission of the author.

FEDERAL SENTENCING GUIDELINES: AN UPDATE ON IMPORTANT NEW INFORMATION SECURITY LIABILITIES

SANFORD SHERIZEN, Ph.D., CISSP
PRESIDENT
Data Security Systems, Inc.
Natick, MA

This analysis contains recommendations on management strategies. Those recommendations are not offered as representing legal advice.

SENIOR MANAGEMENT ALERT

November 1, 1991 will be remembered as a hallmark event for senior executives. On that date, the guidelines which govern the sentencing of organizations convicted of violating federal criminal law went into effect. As a result, the security rules for management changed dramatically.

Previously, senior executives often were able to assign security to someone in the organization and, if there were legal problems, attempt to mount a defense based on the notion that security was not part of their direct responsibility. That "ostrich defense" has been challenged, if not undercut, as a result of the Federal Sentencing Guidelines.

The Federal Sentencing Guidelines contain clear messages that senior management must prevent, detect, and report crimes. According to the Guidelines, "high level personnel" and "substantial authority personnel" now have to explicitly consider crime control as an important responsibility on which they will be judged. Unless an organization has instituted an effective crime control program which meets legal measurement, there could be serious financial and other liabilities affecting individuals as well as organizations.

Management has serious potential legal exposure where organizational misconduct or offenses are found. Punishments include high fines and even corporate probation. Recently, the U.S. Sentencing Commission proposed expanded coverage of the types of crimes covered under the Guidelines to include computer-related acts. This could dramatically increase the number of computer-related cases which already have been processed under the Guidelines.

The message to management is clear. With so much financial crime now computer-based, crime control programs, including computer crime prevention, are an absolute requirement today.

WHAT ARE THE FEDERAL SENTENCING GUIDELINES?

The Federal Sentencing Guidelines are rules for Federal judges on how to provide appropriate punishments for individuals and for organizations violating Federal statutes. The first set of Guidelines were developed by the U. S. Sentencing Commission to establish appropriate punishments for individuals.

After a five-year effort, the Guidelines directed toward organizations went into effect in 1991. The stated goals of these Chapter 8 organizational guidelines were to "provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct."

The Guidelines state that organizations have a responsibility to "maintain internal mechanisms for preventing, detecting, and reporting criminal conduct." These rules apply to corporations, government agencies, not-for-profits, unions, and other organizations. The Sentencing

Commission has suggested that the Guidelines will apply to a majority of all organizations which are convicted of Federal violations.

The Guidelines make an organization potentially liable for all criminal acts of its employees and other agents. Agents of an organization include independent representatives, consultants, brokers and others who are in a position to carry out an organization's functions.

Thus, the Guidelines represent a legal challenge with wide applicability to a variety of organizations and their working personnel. The Guidelines also represent a management challenge on how to survive in an increasingly complex business environment.

WHY ARE THE GUIDELINES IMPORTANT?

The Guidelines clearly establish the Federal Government's growing concern with fighting white collar and other economic crimes. Government is now forcing businesses and other organizations to face the seriousness of these crimes. Ethics statements and policy announcements alone are no longer considered as sufficient. Specific actions and effective programs will be the measure by which an organization will be evaluated. Faulty judgment calls by management and/or an environment which allows such judgments to be made by agents of the organization have the potential to become considered as punishable events.

The Guidelines provide a model program which senior management needs to establish in order to show that crime prevention is an organizational concern. There are now carrots (incentives) and sticks (disincentives) to involve senior management in fighting crime. There are also new requirements which now necessitate organizations to report crime activities rather than to simply let someone go quietly, especially if they are a high executive or if they have committed what could be considered by outsiders as an embarrassing crime.

HOW ARE THE GUIDELINES IMPORTANT TO INFORMATION SECURITY?

Since so many workplace activities are now computer-related and since information is the key resource for many organizations, the computerization of many traditional crimes has become a major problem. In reality, many of the fraud crimes which the Guidelines cover are, in essence, computer crimes, even if they have not been so defined specifically under the law.

More recently, the Guidelines achieved a more direct relationship to information security issues. The Sentencing Commission addressed computer crimes by offering an amendment regarding computer-related crimes. The Commission sent to the Congress Amendment 7, Computer Related Offenses: Theft of Trade Secrets. The amendment has an effective date of November 1, 1997 unless modified or rejected by Congress. According to the Commission, this amendment provides
(a) "more effective punishment" of computer-related offenses; (b) covers an offense of extortion by threats of damage to certain "protected computers"; (c) covers offenses involving economic

espionage and theft of trade secrets; and, (d) provides a minimum guideline sentence of six months' imprisonment for convictions under the Federal computer crime law. The recognition of computer-related offenses can serve to increase the power of the Guidelines to meet this increasing threat.

Even prior to Amendment 7, however, minimum requirements of what the Guidelines define as an effective program to prevent and detect violations of the law also applied to the complexities of the computerized office. Consider, for example, the concept of care in delegating authority. An organization " must have used due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities." Management decisions on access controls, authorization levels, and other essential information security considerations affect who has discretionary authority as well as how organizations structure their control and supervisory mechanisms over employee activities. Given a do-more-with-less emphasis in today's downsized environment, these decisions are critical to keeping an organization from paying large legal as well as other negative business costs.

The Guidelines are only one of a number of legal changes which indicate that computer crime prevention is increasingly becoming a requirement rather than a choice. As computer crime becomes recognized as a dangerous crime, information security will become a focal point for many strategic, legal, and functional issues.

<u>HOW CAN THE FEDERAL SENTENCING GUIDELINES AFFECT ME AND MY ORGANIZATION</u>?

The Federal Sentencing Guidelines, with its serious punishment potential, should create a major change in senior management views. Fines can range up to as much as $290 million as well as corporate probation, where the court supervises an effective compliance program for the organization.

The formula used to determine a fine requires the judge to multiply the "base fine", which is generally determined by the seriousness of the offense, by a multiplier, which is determined by an organization's "culpability score." The "base fine" may consist of the greater of a company's gain, the victim's loss, or a dollar amount corresponding to an "offense level". The "culpability score" is used to determine the range within which the judge can increase or decrease the "base fine".

Federal judges can multiply fines as much as 400% or reduce them by up to 95%, depending upon specific factors, many of which **partially depend upon how an organization has responded to the Guidelines prior to the violation**. Thus, a company could be fined between $250,000 and many millions of additional dollars, depending upon whether it played an active role in promoting the crime and its degree of cooperation with the Government. In addition, there is a possibility for a shareholder suit alleging that the directors and officers were negligent in not taking the simple but important step of developing an effective compliance program that could have saved the company from these problems (and costs).

The "culpability score" starts with 5 points and may be increased based upon the judge's determination of the involvement of top officials, prior violations, and obstruction of justice. The score can be decreased based upon the judge's findings regarding the existence of an effective program to prevent and detect violation, voluntary disclosure to the appropriate authorities, cooperation with an investigation conducted by the appropriate authorities, and acceptance of responsibility by the organization. Further points are considered for the size of the organization and the management tolerance of crime activities.

One of the most effective ways to decrease "culpability scores" and therefore lower financial penalties is to have an effective program to detect and prevent violations of the law. The Guidelines indicate what is required for such a program.

STRUCTURING A PROGRAM TO MEET THE GUIDELINES

In order to fulfill the Guideline requirements, it is best to develop an effective program prior to a violation rather than after a violation has been found. Attorneys have indicated that a strong compliance program may avoid prosecution of the organization altogether, even if an employee does commit an offense. If there is prosecution, an effective program can lead to a reduction in mandatory fines. An effective program may also result in more favorable treatment in certain civil and criminal lawsuits. Finally, a pre-violation program can be structured to meet an organization's values and particular conditions. A post-violation program will have to meet stiff requirements set by the courts and be instituted rapidly as well as in a costly manner. The choice would seem to be evident.

An effective program requires, at a minimum, the following elements (summarized):

> Establish compliance standards and procedures for employees and other agents that are reasonably capable of reducing the prospect of criminal conduct.
>
> Assign a specific high level individual with overall responsibility to oversee compliance with such standards.
>
> Make efforts to avoid delegating substantial discretionary authority to those with propensities to commit crimes.
>
> Develop methods for communicating standards and procedures, such as training programs and publications.

Establish methods for achieving compliance, such as monitoring and auditing programs and/or reporting systems designed so that employees and others can report wrongdoing without fear of retribution.

Create a history of consistent enforcement of standards.

Institute ongoing modifications and improvements to the program when problems appear.

In addition to these program elements, prominent attorneys who are advising on how to meet the Guidelines are suggesting that an inventory of possible legal risks be developed for each organization. While the inventory is not explicitly mentioned in the Guidelines, these attorneys suggest that it is strongly implied. Without getting into the details of this interpretation of the Guidelines, it is important for an organization to conduct an inventory of risks which it faces. Factors to be considered include risks due to the nature of the organization's activities, possible violations that a monitoring program should concentrate upon, and "industry practices" regarding exposure and best practices.

WHAT SHOULD AUDIT, INFORMATION SECURITY, AND MIS PROFESSIONALS DO NOW ABOUT THE GUIDELINES?

The Guidelines offer an opportunity as well as a challenge. The opportunity is that the suggested program is available to serve as a model to meet the requirements of the Guidelines. Information security and audit programs collect aspects of the information needed by those who will coordinate the work of complying with the Guidelines. Further, computer crime prevention must be a key aspect of any crime prevention program today.

On the other hand, the challenge of meeting the Guidelines is similar to the challenge of getting senior management to support information security. Even if it were mandated by law and in their own self-interest, it is often difficult to gain the resources and support from management necessary to make the program effective.

Avoid serious liabilities by reviewing whether your organization meets the Guideline requirements. The following are fundamental steps to be taken to determine whether and how your organization is in compliance:

Conduct a "liability inventory" to determine how your organization could be judged under the Federal Sentencing Guidelines and other legal/ regulatory approaches.

Analyze liability trends in order to determine what emerging problem areas could affect your organization, thus requiring compliance attention.

Determine the most appropriate management strategies which meet compliance requirements.

Evaluate the “implementability” of compliance guidelines, policies, and/or procedures within your organization.

Reinforce compliance and information security awareness messages throughout the organization by means of coordinated information security procedures, employee performance evaluations, management reviews, and other control mechanisms relevant to the Guidelines.

It is important for audit, information security, and MIS professionals to inform their management about the Federal Sentencing Guidelines and to assist as much as possible in establishing crime control efforts throughout the organization. Adequate prevention of crime today can result in substantial savings tomorrow. The assets you save may be your own.

The author would like to thank Jeffrey Kaplan, whose expert writings on the Guidelines are reflected in this analysis. Win Swenson, Deputy General Counsel of the Commission until his recent departure, as well as other Commission personnel were very helpful in providing information. Various information security, EDP audit, MIS and management experts have provided me with responses to an earlier version of this analysis. None of these parties are responsible for any conclusions or interpretations found in this document.

APPENDIX B
LIST OF ACRONYMS

ASIS	American Society for Industrial Security
BCM	Business Case Model
CBA	Cost-Benefit Analysis
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
DISA	Defense Information Systems Agency
DOS	Denial of Service
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
IITUG	International Information Technology Users Group
INFOSEC	Information Security
IRR	Internal Rate of Return
IS	Information Security
ISP	Internet Service Provider
IT	Information Technology
MOE	Measure of Effectiveness
NCC	National Computing Centre
NCCS	National Computer Crime Squad
NPV	Net Present Value
NRIC	Network Reliability and Interoperability Council
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
PSN	Public Switched Network
PSP	Proactive Security Program

PST	Proactive Security Team
RBOC	Regional Bell Operating Company
ROI	Return on Investment
SAIC	Science Applications International Corporation
SATAN	Security Analysis Tool for Administering Networks
TSARS	Telecommunications Security Awareness, Research and Standards
UK	United Kingdom